C3安全峰会
CYBER | CLOUD | COMMUNICATION

全球数据治理态势与中国应对

吴沈括
北京师范大学网络法治国际中心执行主任
联合国网络安全与网络犯罪问题高级顾问
中国信息化百人会数据治理委员会主任
最高人民法院监督咨询专家
邮箱：shenkuo.wu@hotmail.com

作者版权所有
请勿转载

一、新一代信息技术与数据治理相关机遇和风险态势

二、欧盟进路（1）:个人数据与2018年《一般数据保护条例》

三、欧盟进路（2）:非个人数据与2018年《非个人数据自由流动条例》

四、美国进路:欧美数据博弈与2018年《加州消费者隐私法案》

五、数据治理的中国应对

结语：数据治理与企业风控合规

作者版权所有
请勿转载

一、新一代信息技术与数据安全治理相关机遇和风险态势

- 一方面，围绕各类数据的利用，在新一代信息技术的普及应用过程中，人们不断拥抱更多的发展机遇；
- 另一方面，围绕各类数据的保护，我们也面对着来源更为广泛、程度更为深刻的安全风险。

一、新一代信息技术与数据治理相关机遇和风险态势

1、新一代信息技术与数据治理相关机遇

（1）新的技术支持：大数据、人工智能等

（2）新的组织样态：云计算、物联网等

（3）新的应用内容：安保监控、远程诊疗、金融理财、生活娱乐等

一、新一代信息技术与数据治理相关机遇和风险态势

2、新一代信息技术与数据治理风险态势

（1）技术要素风险：木马、病毒、僵尸网络等

（2）组织管理风险：电信网络诈骗等

（3）在线内容风险：色情信息、暴恐信息、虚假信息等

一、新一代信息技术与数据治理相关机遇和风险态势

3、数据治理焦点区域

（1）非刑事责任区域：数据获取、处理（使用）、流转...

（2）刑事责任区域：数据获取、流转、安全事件（泄露）...

二、欧盟进路（1）:个人数据与2018年《一般数据保护条例》

- 2018年5月25日，关于个人数据（个人信息）保护的欧盟新一代制度规范《一般数据保护条例》（简称：GDPR）全面施行。这是欧盟数据治理的里程碑事件，在信息系统和数字经济改造人类生活的时代大潮下，其超越成员国个别立法、统一个人数据保护路径、改变个人数据流转走向，进而深度修正欧盟数据治理的规范趋势，也对全球数据治理生态产生广泛、深刻的影响。
- 对于我国各类主体（包括网络企业）而言，首先需要正视的是，GDPR对于欧盟境外的数据治理格局所带来的重大发展。尤其是其明确规定即使是欧盟境外的主体在特定条件下也必须遵循GDPR的相关规范，这在数字化业务乃至交易形式日趋多样化的技术背景下，迫使我们必须考虑、评估GDPR的适用可能性及其实际影响力。

二、欧盟进路（1）:个人数据与2018年《一般数据保护条例》

1、GDPR的基本价值诉求

2、基本框架与制度要点

3、GDPR制度落地与影响

4、GDPR实施与数据跨境

1、GDPR的基本价值诉求

- 1.1、建设现代化的个人数据治理规范机制、确保欧盟公民和居民对于自身个人数据享有充分的控制权，同时通过协调、简化现行的“数字单一市场”体系在欧盟体制内建设统一的规范框架进一步改善监管环境，以期降低个人数据处理主体的合规风控成本，进而助益包括跨国企业在内的商业主体的业务运营。
- 1.2、在欧盟现行政策法律框架下，个人数据保护问题一贯被统摄于欧盟“数字单一市场”建设进程中，与其他元素共同服务于欧盟在数字经济中谋求世界级领袖地位的总体布局。
- 1.3、并非孤立的制度安排，而是与欧盟《2016年网络与信息系统安全指令》形成欧盟网络法制框架的“双剑合璧”，借以在网络系统安全和基本权利保障两个层面通过灵活的变化组合实现欧盟网络治理的多维战略意图。

2、基本框架与制度要点

- **2.1、宏观架构**：对多样化的利益诉求（公民权利、经济自由、数据主权、公共安全等）有着弹性、动态的取舍衡平，由此决定了总体规范特色：（1）强化个人的权利内容；（2）突出欧盟内部市场的价值位阶；（3）提升规范落实的保障能力；以及（4）改进个人数据跨境传输的流程管控并建构全球数据保护标准。

- **2.2、微观设计**：
  1. 欧盟个人数据治理的制度规范将扩展适用于处理欧盟公民和居民个人数据的所有外国主体；
  2. 为应对数字经济发展、数据价值日增的新技术趋势，引入了一系列新型“数字权利”，包括被遗忘权、数据可携权等；
  3. 还引入极为严格的数据保护合规要求，并通过最高处罚为涉事主体全球营收总额4%的惩罚机制予以强化。

3、GDPR制度落地与影响

主要国际影响包括：

1. 对网络新技术新应用研发造成重大影响，尤其是大数据、云计算以及人工智能等深度依赖数据处理的新业务样态将承受GDPR的规范约束；

2. 对包括中国企业在内的全球数据处理主体的业务运营模式造成重大影响，尤其是GDPR引入“设计隐私（Privacy by Design）”数据保护机制，使得域外主体在业务合规过程中被迫接受欧盟数据治理理念；

3. 对国际数据治理生态造成重大影响，特别是GDPR以个人数据跨境制度为有力抓手，直接制约了他国的数据治理制度建设。

4、GDPR实施与数据跨境

4.1、“充分性”认定机制：日本、韩国、加拿大

4.2、双边数据保护协定：美国、英国、印度

4.3、多边数据保护框架：联合国、欧洲委员会（CoE）

作者版权所有
请勿转载

三、欧盟进路（2）:非个人数据与2018年《非个人数据自由流动条例》

1、欧盟非个人数据本地化要求图景

2、欧盟非个人数据治理的立法要旨

3、欧盟非个人数据流动的治理立场

作者版权所有
请勿转载

2017年下半年，欧盟发布了关于《非个人数据自由流动条例》的提案，为非个人数据的流转提出了新指导性规则。该提案在修订后于2018年10月4日由欧洲议会正式通过，最新发布的文本属第47号修订版，其对提案的内容作了必要的删除与新增。

《非个人数据自由流动条例》(2018-10-04)

第1条 主旨事项

第2条 适用范围

第3条 定义

第4条 欧盟内数据自由流动

第5条 有权机关获取数据

第6条 数据迁移

第7条 机关间合作程序

第8条 评估和指南

第9条 最终条款

1、欧盟非个人数据本地化要求图景

数据本地化措施的规定与执行方式非常丰富，在不同的成员国内有不同的规定。据分析，截止2017年，已有大约60-65种已知措施，且在后续欧盟的评估过程中，被认定为明显不合理或显失比例的，约占被评估措施的三分之二。这其中，并非每一种措施都被规定在法律规定中，有一些措施的机制表现形式则是通过学术性理论提出进而影响法律未做相关规定的地方。

作者版权所有
请勿转载

1、欧盟非个人数据本地化要求图景

数据本地化问题的成因主要包括：

1、行政或立法举措导致在数据主动控制区域以外的范围被阻隔；

2、因法律不确定性以及监管机构等公共机构对监管数据可用性的不信任

问题驱动了数据本地化措施的施行。

2、欧盟非个人数据治理的立法要旨：立法目标

非个人数据流转的总体目标在《非个人数据流动条例》中得以体现，其提出了亟待解决的问题：

（1）改善数字单一市场中跨境的非个人数据的流动性；

（2）确保有权机关为监管控制目的要求和接收数据的权力不受影响；

（3）使数据存储或其他处理服务的专业用户更容易切换服务提供商和端口数据，同时避免为服务提供商带来过度负担以及扭曲市场。

3、欧盟非个人数据流动的治理立场

（1）数据服务的广义适用：数据本地化的限制

反映了欧盟相关部门在非个人数据流转问题上的治理立场——数据存储以及数据处理等服务应当在广义上被应用，尽可能实现各类IT系统包括云类服务在内的技术的物尽其用。

3、欧盟非个人数据流动的治理立场

（2）消除贸易障碍与竞争扭曲：提高法律确定性与可操作性

通过在成员国之间建立一个明确的框架并与会员国进行合作，以及通过自律，该条例旨在提高法律确定性和提高信任水平，同时由于合作的灵活性，基于成员国的单一联络点，长期保持相关性和有效性框架。

欧盟数据安全治理框架图景：

《网络与信息系统安全指令》（Network Security Directive）

《一般数据保护条例》（GDPR）2018

《非个人数据自由流动条例》（Non Personal Data）2018

《电子隐私条例》（E-Privacy）2019

《电子证据条例》（E-Evidence）2019

《网络安全法案》2019

……

作者版权所有
请勿转载

四、美国进路:欧美数据博弈与2018年《加州消费者隐私法案》

（一） 系统明确的规范体系

（二） 清晰可行的落实配套

（三） 务实便利的权利实现

2018年《加州消费者隐私法案》立法背景

1、个人信息利用的技术经济现实

2、个人信息治理的法律规范困境

3、个人信息侵害的突发非常事件

4、个人信息保护的公众价值期待

作者版权所有
请勿转载

（一） 系统明确的规范体系

1、以体系协调为制度逻辑起点

2、以控制、透明为制度价值核心

3、以细分权能为制度框架主轴

4、以处理规则为制度设计依托

5、以权益衡量为制度安排特色

作者版权所有
请勿转载

1、以体系协调为制度逻辑起点

……加利福尼亚州宪法赋予一项隐私权。现行法律明确各种情境下个人信息的保密性要求，并且规定企业或者个人在其含个人信息的计算机数据遭受安全侵害时按规定披露侵害事实。

……本法案就民法典有关隐私的第三篇第四部分增加第1.81.5章（自第1798.100节始）。

……法案禁止上述规定限制企业遵守联邦、州或地方法律等规范的能力。

2、以控制、透明为制度价值核心

人们希望获得隐私并可以更多地控制自己的个人信息。加利福尼亚州的消费者应该能够控制他们的个人信息，并且他们希望确保有保护措施防止滥用其个人信息。企业既可以尊重消费者的隐私，也可以为他们的商业行为提供高水平的透明度。

3、以细分权能为制度框架主轴

（i）因此，立法机关的意图是通过确保以下权利，为消费者提供控制其个人信息的有效方式，从而进一步加强加州人的隐私权：

（1）加利福尼亚人有权知道正在收集哪些个人信息。

（2）加利福尼亚州的人有权知道他们的个人信息是否被出售或披露，以及出售或者披露给谁。

（3）加州人有权拒绝出售个人信息。

（4）加州人有权访问他们的个人信息。

（5）即使加利福尼亚人行使其隐私权，也享有平等获得服务和价格的权利。

4、以处理规则为制度设计依托

（1）收集

（2）处理

（3）出售

（4）披露

（5）保留

（6）共享；等等

作者版权所有
请勿转载

5、以权益衡量为制度安排特色

（d）如果企业或服务提供商有必要维护消费者个人信息的，其不应被要求遵守消费者请求删除其个人信息的规定，以便：

（1）完成收集个人信息的交易，提供消费者要求的商品或服务，或者在企业与消费者正在进行的业务关系场景中可合理地预期，或以其他方式履行企业与消费者之间的合同义务。

（2）检测安全事件，防止恶意的、欺骗的、虚假的或非法活动;或起诉那些对此活动负责的人。

（3）调试以识别和修复因损害现有预期功能而产生的错误。

（4）行使言论自由，确保其他消费者行使言论自由的权利，或行使法律规定的其他权利。

（5）遵守《刑法》第2部分第12标题项下第3.6章（从第1546节开始）《加州电子通信隐私法》。

（6）参与公开的或有同行评审的科学、历史或统计研究符合所有适用的道德和隐私法律的公共利益，如果企业删除信息可能导致研究成果难以实现或遭到严重损害的（消费者已提供了知情同意）。

（7）仅仅用于企业内部，该使用是根据消费者与企业的关系，使消费者拥有该等合理期待。

（8）遵守法定义务。

（9）在内部以其他合法方式使用消费者的个人信息，该方式与消费者提供其信息的场景相匹配。

作者版权所有
请勿转载

（二） 清晰可行的落实配套

1、公力监管兼以私权救济

2、权利宣示兼以程序设定

作者版权所有
请勿转载

1、公力监管兼以私权救济

……本法案的规定由州总检察长根据相关规范负责执行，并赋予诉讼私权以应对未经授权的访问和泄露、盗窃或披露消费者未加密或未编辑个人信息等特定行为。

……1972年，加利福尼亚选民修改了《加利福尼亚州宪法》，将隐私权纳为全体人民“不可剥夺”的权利之一。该修正案赋予每位加利福尼亚州人法定且可执行的隐私权。

……个人就其个人信息的使用包括销售的控制能力对于该隐私权而言具有基础性意义。

……由于加利福尼亚选民批准了隐私权，加利福尼亚州立法机关采取特别机制以保护加利福尼亚人的隐私，其中包括《在线隐私保护法案》、《数字世界加利福尼亚未成年人隐私权法案》以及《阳光法案》，后者旨在向加利福尼亚人指明企业处理消费者个人信息过程中的“何人、何物、何地与何时”信息。

2、权利宣示兼以程序设定

1798.120（a）消费者有权在任何时候指示一个欲将消费者个人信息出售给第三方的企业不得出售该消费者的个人信息。这项权利可以被称为“选择退出”权。

（b）向第三方出售消费者个人信息的企业应根据第1798.135节第（a）条的规定向消费者发出通知，告知消费者该信息可能会被出售并且消费者有权选择不出售他们的个人信息。

（c）如果一家企业从消费者那里收到指示不得出售其个人信息，或者出售小部分消费者的个人信息没有得到该部分消费者同意的情况下，根据第1798.135节第（a）条第4款的规定，出售这部分消费者信息的行为应该被禁止，直到收到消费者指示后方可进行，除非消费者随后明确授权可出售其个人信息。

（d）尽管有第（a）条规定，如果企业实际明知消费者年龄小于16岁，企业不应出售该消费者的个人信息，除非消费者的年龄是在13至16岁之间，或父母或监护人已明确授权企业可以出售年龄小于13岁的消费者个人信息。企业任何故意忽视消费者年龄的行为应被视为其已明确知晓该消费者年龄。这一权利可以被称为“选择加入”权。

作者版权所有
请勿转载

2、权利宣示兼以程序设定

（2）在收到消费者的请求且经核实后45天内向消费者免费披露并向其提供所需信息。企业应立即采取措施确定该请求是否可经验证，但这不因此延长企业在收到消费者请求后的45天内披露和提供信息的义务。只有在合理必要的情况下，企业提供消费者所需信息的时间段可再延长45天，但前提是在第一个45天期限内企业向消费者发出了延期通知。披露应涵盖企业收到经核实的请求之前的12个月，并应以书面形式提交，如果消费者持有该企业的用户账户，则应通过消费者的用户账户来交付，如果消费者未开设该企业的用户账户的，则通过邮件或其他消费者自行选择的电子方式来交付，但无论如何都应有一种便捷有效的方式允许消费者在不受阻碍的情况下将这些信息从一个实体传输到另一个实体。企业不应以提出需经核实请求为由，要求消费者创建该企业的用户账户。

（三） 务实便利的权利实现

1、明晰的作为义务设定

2、合理的权利实现保障

3、经济的权利实现渠道

4、严密的责任追究机制

作者版权所有
请勿转载

1、明晰的作为义务设定

企业从可验证的消费者处接收到要求访问个人信息的请求后，应立即采取措施向消费者免费披露和提供本节所要求的个人信息。个人信息的提供可通过邮件或电子方式，如果以电子方式提供，信息应以便携式方式提供，并且在技术上是可行的，且采用易于使用的格式，允许消费者无障碍地将此信息传输给其他实体。企业可以随时向消费者提供个人信息，但在12个月内不应被要求向同一位消费者提供两次以上的个人信息。

2、合理的权利实现保障

1798.125 （a）（1）企业不得因为消费者行使本标题下任何消费者的权利而歧视消费者，包括但不限于：

（A）拒绝向消费者提供商品或服务。

（B）对商品或服务收取不同的价格或费率，包括通过给予不同的折扣、其他福利或处罚。

（C）如果消费者行使本标题项下消费者的权利，向消费者提供不同等级或质量的商品或服务。

（D）提示消费者将获得不同价格或费率的商品或服务，或者将向消费者提供不同水平或质量的商品或服务。

3、经济的权利实现渠道

1798.135 （a）需要遵守第1798.120节规定的企业，应采取消费者可合理获取的形式：

（1）在其互联网主页上提供一个清晰且明显的，命名为“不得出售我的个人信息”的链接，使消费者或经消费者授权的人可以选择不出售消费者的个人信息。企业不应为了指示不出售消费者的个人信息而要求消费者创建用户账户。

（2）根据第1798.120节的规定，制作关于消费者权利的描述，同时在如下界面中有一个单独的“不得出售我的个人信息”的链接：

（A）如果企业拥有在线隐私政策的话，则在线隐私政策中要有链接。

（B）在任何加利福尼亚州对消费者隐私权的具体描述中要有链接。

4、严密的责任追究机制

1798.150（a）（1）任何消费者如其在第1798.81.5节（d）条（1）款（A）项下所定义的未加密或未经处理的个人信息，由于企业违反义务而未实施和维护合理安全程序以及采取与信息性质相符的做法来保护个人信息，从而遭受了未经授权的访问和泄露、盗窃或披露，则消费者可因以下任何一项而提起民事诉讼：

（A）为每个消费者每次事件赔偿不少于一百美元（100美元）且不超过七百五十美元（750美元）的损害赔偿金或实际损害赔偿金，以数额较大者为准。

（B）禁止令或宣告性法律救济。

（C）法院认为适当的任何其他救济。

（2）在评估法定损害赔偿金额时，法院应考虑案件任何一方提出的任何一种或多种相关情况，包括但不限于不当行为的性质和严重性、违法行为数量，持续存在的不当行为，发生不当行为的时间长短，被告的不当行为的故意以及被告的资产、负债和净值。

注：数据治理的美国路线图

联邦层面的统一立法：类似于欧盟GDPR?

作者版权所有
请勿转载

数据治理欧美方案的路径差异

1、对内（数据流转）

欧盟：“Opt-in”机制

美国：“Opt-out”机制

2、对外（数据跨境）

欧盟:抬高他国数据管控基线

美国:拉低他国数据管控基线

五、数据治理的中国路径

1、政策战略

2、法律规范

3、其他规范

（1）国家网信部门

（2）最高司法机关

作者版权所有
请勿转载

五、数据治理的中国路径

A、政策战略

1. “互联网+”行动计划
2. 中国制造2025
3. 《关于促进大数据发展行动纲要》
4. 网络强国战略
5. 《“十三五”国家信息化规划》
6. 《国家网络空间安全战略》
7. 《网络空间国际合作战略》
8. 《新一代人工智能发展规划》

作者版权所有
请勿转载

五、数据治理的中国路径

B、法律规范

- 网络安全法
- 电子商务法
- 个人信息保护法（拟）
- 数据安全法（拟）
- 电信法（拟）

作者版权所有
请勿转载

五、数据治理的中国路径

C、其他规范

（1）国家网信部门

1. “微信十条” (2014.08.07)
2. “约谈十条” (2015.04.28)
3. “直播规定”(2016.11.04)
4. “网安标准化工作意见”(2016.08.12)
5. 网络产品和服务安全审查办法（试行） (2017.05.02)
6. 互联网新闻信息服务管理规定（2017.06.01）
7. 互联网信息内容管理行政执法程序规定（2017.06.01）
8. 个人信息和重要数据出境安全评估办法（征求意见稿） (2017.04.11)
9. 关键信息基础设施安全保护条例（征求意见稿） (2017.7.11）*
10. 个人信息安全规范 - 国家推荐标准

五、数据治理的中国路径

C、其他规范

（2）最高司法机关

1.“两高一部”电信网络诈骗《意见》(2016.12.20)

2.“两高”侵犯公民个人信息刑事司法解释（2017.06.01）

3.“两高”扰乱无线电通讯管理秩序刑事司法解释（2017.07.01）

4.“两高”关于网络犯罪的司法解释（2018）

五、数据治理的中国路径

应对前瞻：

（一）全面动态的全球规则演进研判

（二）价值清晰的顶层设计框架建构

（三）系统可行的差别规范制度安排

（四）经济便利的权利责任落实途径

作者版权所有
请勿转载

主要启示：

（一）安全理念的转变

（二）风控策略的设定

（三）核心权益的维护

（四）关键风险的管控

作者版权所有
请勿转载

结语：数据治理与企业风控合规

（一）安全理念的转变

新理念：“设计安全”(Security by design)

作者版权所有
请勿转载

结语：数据治理与企业风控合规

（二）风控策略的设定

1.消极维度

互联网企业自身遵循法律条文引入的各行为规范从而确保免受法律处罚

2.积极维度

根据法律规范授权发现、纠正侵害互联网企业乃至互联网产业利益的不合规行为

结语：数据治理与企业风控合规

（三）核心权益的维护

《网安法》第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

结语：数据治理与企业风控合规

（三）核心权益的维护

1.注意法律规范的体系化综合运用；

2.充分利用法律赋予的正当化机制。

作者版权所有
请勿转载

结语：数据治理与企业风控合规

（四）关键风险的管控

1.《网安法》第六十三条 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

2.“单位犯（...）罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照（...）的规定处罚。”

结语：数据治理与企业风控合规

（四）关键风险的管控

“责任阻断机制”建设

1.横向：定岗定人，明确厘定行为人主观认识与客观行为的边界；

2.纵向：定岗定责，界分业务作业层级切断单位法律责任因果链。

谢谢！

吴沈括
北京师范大学网络法治国际中心执行主任
联合国网络安全与网络犯罪问题高级顾问
中国信息化百人会数据治理委员会主任
最高人民法院监督咨询专家
邮箱 shenkuo.wu@hotmail.com

作者版权所有
请勿转载